

**APPLICATION FOR
UNITED STATES PATENT
IN THE NAME OF**

ROBERT ADAMS AND JOSE P. PUTHENKULAM

FOR

CONTROL OF ACCESS CONTROL LISTS BASED ON SOCIAL NETWORKS

Prepared By:

PILLSBURY MADISON & SUTRO LLP

Ninth Floor, East Tower

1100 New York Avenue, N.W.

Washington, D.C. 20005-3918

Telephone (213) 488-7100

Facsimile (213) 629-1033

Attorney Docket No: 81674-273215

Client Reference No.: P-9895

Express Mail No. EL 669 015 805 US

TITLE OF THE INVENTION

CONTROL OF ACCESS CONTROL LISTS BASED ON SOCIAL NETWORKS

BACKGROUND OF THE INVENTION

5 1. Field of the Invention

The present invention generally relates to management of access control lists (ACLs) used to regulate access to shared resources. More particularly, the present invention relates to automated control of ACLs based on analysis of social networks to regulate access.

10 2. Discussion of the Related Art

In large institutions such as corporations, research centers, and educational facilities, networked computer systems are commonplace. By utilizing a network architecture, various resources within the institution may be shared by its users. For example, all the users having workstations located at the northwest end of a floor in a building could be configured to share a common printer. Or, all the users on a design team may be granted access to open/read a spreadsheet file, containing all the names and telephone numbers of the team members, stored on the workstation of a particular user or system.

Typically, access to files and other resources are managed with access control lists (ACLs), which contain information such as an identity (e.g., user name, identification number, etc.) of the user or entity, and an access right or level (e.g., no access, read-only access, read/write access, etc.), for all the users/entities that have access to a particular resource. These ACLs are usually manually configured by a user or a system administrator, and stored on an authentication server. That is, the identity and access right pairs are manually entered to create

the ACLs for each shared resource in a network. However, the ACLs may be stored as part of the resource itself, or separately. In a file system, for example, the ACLs are typically stored as part of the file resource itself. In a case where the resource is a printer, for example, the ACLs are stored usually on a server running the Print Scheduler.

5 Manual entry of ACLs is a long and cumbersome process, which increases the maintenance costs of the entire system, particularly when new groups are formed or disbanded over short periods of time. Additionally, when a new user transitions into a group, or transitions from one group to another, a number of ACLs may be affected. Time is required for a user or a system administrator to update each affected ACL so that the new user has the appropriate access
10 to the shared resources utilized by the group (or even to restrict access to shared resources of a former group). Access control lists can also become very large and unwieldy, which makes it difficult to remember which users are on the ACLs, or to whom the access levels have been assigned. Therefore, automated, fast, accurate, and cost-effective management of ACLs for shared resources in a network infrastructure is desirable.

BRIEF DESCRIPTION OF THE DRAWINGS

15 Fig. 1 illustrates a social network utilizing an access control list (ACL) to control access for a shared resource according to an embodiment of the present invention;

Fig. 2 illustrates a flow chart diagram showing an operation of a social network utilizing
20 an access control list (ACL) to control access for a shared resource according to an embodiment of the present invention;

Fig. 3A illustrates a flow chart diagram showing the determining of social network data from communications to and from a user according to an embodiment of the present invention; and

Fig. 3B illustrates a flow chart diagram showing the determining of an access level for a user based on social network data according to an embodiment of the present invention.

DETAILED DESCRIPTION

Fig. 1 illustrates a social network utilizing an access control list (ACL) to control access for a shared resource according to an embodiment of the present invention. A plurality of users or entities (A-E) 110, 112, 114, 116, 118 are shown having communications with a user or entity 120 having the shared resource 170. For example, the plurality of users 110, 112, 114, 116, 118, 120 may all be co-workers in the same company, or only the co-workers working together on a particular project. The shared resource 170 may include a file, a directory, an input/output device, a piece of hardware (e.g., a printer, copier, storage device), and a computer system (such as portable electronic devices like personal digital assistants (PDAs), cellular telephones, and Internet appliances, etc.). Other shared resources 170 may include other electronic systems, such as electronic banner systems, digital cameras, remote-controlled devices, etc. This web of personal relationships among the users 110, 112, 114, 116, 118, 120 is referred to as a social network. Each user 110, 112, 114, 116, 118 having communications with the user 120 having the shared resource 170 may each have various degrees of interaction with the user 120 (as well as with each other). For example, some users may communicate more often to a particular user than others. In the example illustrated in Fig. 1, only a single user 120 having a single shared resource 170 is shown. However, the social network may be more complex, wherein the users

110, 112, 114, 116, 118 also have communications amongst each other, and each one of the users has shared resources that may be shared with the entire group. In the example illustrated in Fig. 1, users A-E 110, 112, 114, 116, 118 make up the social network around the user 120 having the shared resource 170.

5 A social network monitor 130 is provided to monitor the communications between the plurality of users 110, 112, 114, 116, 118 and the user 120 having the shared resource 170. Many forms of communication may be exchanged between the users (A-E) 110, 112, 114, 116, 118 and the user 120 having the shared resource 170. E-mail communications are one of the most popular forms of electronic communication. For example, the social network monitor 130
10 may be a software application residing on a computer system of the user 120 having the shared resource 170 (or at any other suitable location, or with any other suitable user or system) that monitors all e-mail traffic entering and leaving the computer system of the user 120 having the shared resource 170. The software application may be stored on any suitable computer-readable medium, such as a semiconductor memory, a hard disk drive, an optical disk, or a magnetic tape,
15 etc. However, any form of communication between the users 110, 112, 114, 116, 118, 120 may be monitored, such as file transfers, instant messages, commands sent from one computer system to another, etc.

By monitoring the communications between the users 110, 112, 114, 116, 118, 120 in the social network, the social network monitor 130 may determine social network data therefrom.

20 Social network data may include any information utilized to construct the social network model and assign access levels amongst the users 110, 112, 114, 116, 118 to access the shared resource 170. For example, the social network data extracted from the communications between the users 110, 112, 114, 116, 118, 120 may include: (1) identities (names, identification numbers, etc.) of

the users 110, 112, 114, 116, 118, 120; (2) the frequency of interaction over a time period between the users 110, 112, 114, 116, 118, 120; (3) a chronology of the communications (e.g., date and time of each communication, how recent was the last communication); (4) a topic of the communications; (5) a ratio of received/transmitted communications between particular users; and (6) any resources (e.g., attached files) included in the communications. For example, the social network data may indicate that user B 112 exchanged 17 e-mails with the user 120 having the shared resource 170 over a 24-hour period, while user C exchanged only 3 e-mails with the user 120 having the shared resource 170 over the same period. However, social network data may be inferred from sources other than e-mail communications, such as organizational groupings, locality (based on where people are physically located), family information, Web page access monitoring, telephone conversation monitoring, chat room monitoring, etc.

A social network access controller 140 is provided to determine, based on the social network data, an access level for the user to access the shared resource 170. The social network access controller 140 may be in the form of a software application executing on a computer system, for example, of the user 120 having the shared resource 170. Likewise the social network monitor 130 may also be on the computer system of the user 120 having the shared resource 170. However, the social network monitor 130 and the social network access controller 140 may reside on separate systems as well.

Different access levels may be assigned to each one of the users 110, 112, 114, 116, 118 based on the social network data determined for each user 110, 112, 114, 116, 118. For example, the access levels for a computer file resource 170 (such as a Microsoft Word document, or a hypertext markup language (HTML) file) may include: (1) no access — the user is barred from accessing the resource 170; (2) read-only access — the user can only read the file; (4) read/write

access — the user can read and write to the file; (5) execute access — the user can execute (run) the file, or files in a directory; (6) create access — the user can create a new file in a directory; (7) owner access — the user can modify the file, directory, etc.; (8) all access — the user has access to all read, write, execute, and create functions to the resource (file) 170; and (9) control
5 access — the user has access to control a remote-controlled device resource 170, including, for example, remotely closing and opening physical doors. However, there may be other access level types as well, such as the ability to change a paper type in a paper tray (e.g., from draft paper to bonded paper) in a shared printer resource 170. For a chat room or bulletin board service application, various access types may include permissions to add, invite, or ban users;
10 permissions to view and/or write posted messages (bulletins); or permissions to run scripts or programs within the chat rooms.

By utilizing the social network data based on a set of defined rules, various access levels may be automatically configured for each user 110, 112, 114, 116, 118. For example, the access levels may follow a rule-set based on the type and/or frequency of interaction (communications)
15 between the users 110, 112, 114, 116, 118, 120 as follows:

TABLE 1

<u>Social Interaction Type (Frequency) Determined from Social Network Data</u>	<u>Access Level</u>
Frequent e-mail communication, >10 per week	all access
E-mail communication at >3 per week	read/write access and execute access
E-mail communication at least once in two weeks	read-only access and execute access
E-mail communication at least once a month	read-only access
All other cases	no access

However, the frequency of communication is but one possible criteria that may be extracted from the social network data to determine access levels. For example, access levels may be granted based on the topics mentioned in the communications between the users 110, 112, 114, 116, 118, 120. That is, the communications may be monitored so as to search for particular keyword(s). Then, access levels may be granted based on the number of occurrences of these particular keyword(s). The various access levels may be granted depending on the number of occurrences (i.e., the more times a specific keyword(s) is found in a communication, the higher level of access is granted). Different weights may be assigned to different keywords, so that certain keywords may have higher weights than others (thus leading to higher access levels). For example, a “point” system may be utilized to keep track of the number of points accumulated based on the occurrence of keywords detected in communications within a period of time. Access levels may also be determined by the user’s identity (e.g., certain users are preset to have minimum access levels), the chronology of the communications (e.g., users having more recent communications are granted higher access levels than users having less recent communications), or the resources (such as a particular file, type of file, a Web page, a document, etc.) transmitted to and/or received from the user. Access levels may also be determined by a user’s interest in the shared resource 170, such that the greater the interest in the shared resource 170 (e.g., the greater the frequency of accessing the shared resource), the higher access level may be provided over time.

The social network access controller 140 also configures an access control list (ACL) 150, which is used to provide a user with the determined access level for accessing the shared resource 170. The social network access controller 140 is preferably adapted to add or remove identity entries as well, as new users or entities transition into and out of a group. That is, the

social network monitor 130 notifies the social network access controller 140 when the user 120 having the shared resource 170 receives or transmits communications to a new user or entity, and a new identity entry may be ultimately added to the ACL 150. As mentioned above, the ACL 150 preferably includes an identity and access right pair. That is, a user name and an access
5 level may be associated in the ACL 150, for example:

- (1) John Doe, read-only access;
- (2) Jane Wright, read/write access; and
- (3) Jose Paul, all access.

By looking-up the access control list 150, a shared resource provider 160 is adapted to
10 provide to the user 110 who is attempting to access the shared resource 170 the appropriate access level, and restrict access, if required. The ACL 150 may contain only the identity/access level pair information, or it may contain other information as well, such as a password to provide more precise access control based on the password(s) provided by the user.

The shared resource provider 160 may be a software application resident on the computer
15 system of the user 120 having the shared resource 170, or on a separate system, such as on the system storing the shared resource 170 if the shared resource 170 is stored separately from the computer system of the user 120 “having” the shared resource 170. This is particularly the case if the shared resource 170 (which may be a plurality of files, for example) is distributed across a network. The shared resource provider 160 acts as a gateway to check the ACL 150 and provide
20 the appropriate level of access to the user(s) attempting to access the shared resource 170. The shared resource provider 160 is preferably implemented as part of, for example, the file system that controls the opening, reading, and writing accesses of the shared resource 170. Therefore, if the shared resource 170 is a computer file and if the ACL 150 shows that user A 110 has a “read-

only” access level, then, the shared resource provider 160 will only enable user A 110 to read the shared resource file 170 and nothing else.

Fig. 2 illustrates a flow chart diagram showing an operation of a social network utilizing an access control list (ACL) to control access for a shared resource according to an embodiment of the present invention. First, communications between a user(s) 110, 112, 114, 116, 118 and a user or entity 120 having a shared resource 170 are monitored 210. Based on the communications between user(s) 110, 112, 114, 116, 118 and a user 120 having a shared resource 170, social network data is determined 220. As shown in Fig. 3A, for example, e-mail communications to a user 110, 112, 114, 116, 118 from the user 120 having the shared resource 170 are identified 310. E-mail communications from a user 110, 112, 114, 116, 118 to the user 120 having the shared resource 170 are also identified 320. The e-mail communications to and from the user 120 having the shared resource 170 with a particular user 110, 112, 114, 116, 118 are counted 330.

From the social network data (e.g., the number of e-mail communications to and from a particular user 110, 112, 114, 116, 118 with the user 120 having the shared resource 170), an access level is determined 230 for each user 110, 112, 114, 116, 118 regarding access to the shared resource 170. As shown in Fig. 3B, for example, the number of e-mail communications counted to and from the user 120 having the shared resource 170 with a particular user 110, 112, 114, 116, 118 is obtained 340. Then, as mentioned above for example, the number obtained may be compared to a look-up table (see Table 1 above) to determine 350 the access level for a particular user 110, 112, 114, 116, 118. An appropriate access level may be assigned 360 to the user 110, 112, 114, 116, 118 based on the look-up table. Once the access level is determined

230, an access control list (ACL) 150 for the shared resource 170 is configured 240 so as to provide the appropriate access level for each user capable of accessing the shared resource 170.

Therefore, the management of ACLs according to an embodiment of the present invention is automated and cost-effective, allowing a resource 170 to be shared with a dynamic “social” group. That is, the resource 170 may be shared with a group (social network) that is constantly changing. Additionally, the ACLs may be managed and updated continuously (and “on-the-fly” each time the users 110, 112, 114, 116, 118, 120 communicate amongst each other or attempt to access the shared resource 170), so as to add or remove entries (of users) or change access levels in the ACL 150 as users transition in and out of a group, or as the communications between the users change (in frequency, topic matter, etc.).

While the description above refers to particular embodiments of the present invention, it will be understood that many modifications may be made without departing from the spirit thereof. The accompanying claims are intended to cover such modifications as would fall within the true scope and spirit of the present invention. The presently disclosed embodiments are therefore to be considered in all respects as illustrative and not restrictive, the scope of the invention being indicated by the appended claims, rather than the foregoing description, and all changes that come within the meaning and range of equivalency of the claims are therefore intended to be embraced therein.